

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-51951

(P2001-51951A)

(43) 公開日 平成13年2月23日 (2001.2.23)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z 5 B 0 8 5
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 Z 5 J 1 0 4
			9 A 0 0 1

審査請求 未請求 請求項の数 5 O L (全 8 頁)

(21) 出願番号 特願平11-229542

(22) 出願日 平成11年8月16日 (1999.8.16)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 橋本 正一

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72) 発明者 中原 慎一

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100087848

弁理士 小笠原 吉義 (外1名)

最終頁に続く

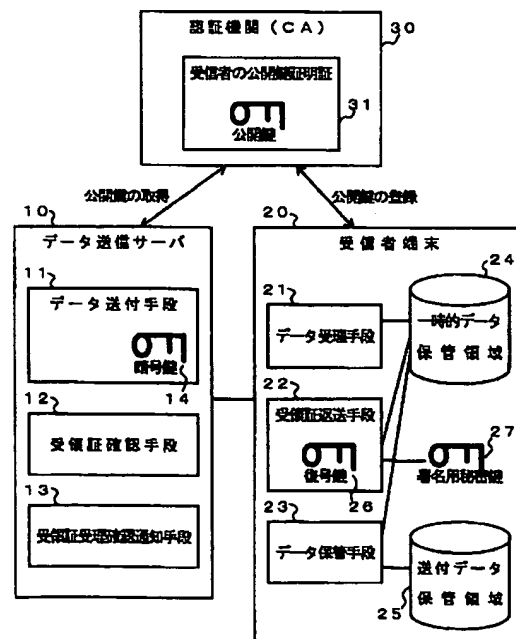
(54) 【発明の名称】 電子データ配送システム、電子データ配送方法、電子データの受信者端末およびその受信者端末用プログラム記録媒体

(57) 【要約】

【課題】 電子データ配送システムにおいて、ネットワークを介してデータを配送する際に、送信者が受信者から送付データの受領を証明する情報を受け取らない限り、受信者が受領した送付データの内容を確認できないようにする。

【解決手段】 データ送信サーバ10が、暗号鍵14を用いて暗号化した送付データを送ると、受信者端末20は、それを受領して一時的データ保管領域24に保管し、受領証返送手段22によって受信者に知られない方法により組み込まれた復号鍵26を用いて送付データを復号し、それに対して電子署名を生成し受領証として返送する。データ送信サーバ10は、受領証を確認すると、受領証受理確認通知を受信者端末20に送付する。受信者端末20は、受領証受理確認通知を受領後、暗号化された送付データを復号鍵26を用いて再度復号し、送付データ保管領域25に保管して、受信者がその内容を確認できるようにする。

本発明のシステム構成例



【特許請求の範囲】

【請求項1】 データ送信サーバと受信者端末とを有し、コンピュータネットワークを介して確かに電子データを送付したことの証拠情報を、データ送信サーバが受信者端末から受け取るための情報処理システムであって、前記データ送信サーバは、送付データを暗号鍵によって暗号化して、暗号化データを受信者端末へ送付するデータ送付手段と、前記受信者端末から受領証を受け取る受領証確認手段と、受領証を受領したことを受信者端末へ通知する受領証受理確認通知手段とを備え、前記受信者端末は、受理した暗号化データを一時的データ保管領域に一時的に保管するデータ受理手段と、受信者に知られない方法により組み込まれた復号鍵を用いて、受信者が内容を確認できない態様で前記受理した暗号化データを復号し、復号された送付データに対して、受領証となる電子署名を生成するための署名用秘密鍵を用いて受領証を作成し、前記データ送信サーバへ返送する受領証返送手段と、前記データ送信サーバから受領証受理確認通知を受け取った後に、前記暗号化データを復号鍵を用いて復号し、受信者が内容を確認できる態様で送付データ保管領域に復号した送付データを保管するデータ保管手段とを備えることを特徴とする電子データ配送システム。

【請求項2】 データ送信サーバと受信者端末とを有し、コンピュータネットワークを介して確かに電子データを送付したことの証拠情報を、データ送信サーバが受信者端末から受け取るための情報処理システムにおける電子データ配送方法であって、前記データ送信サーバは、送付データを該データ送信サーバ内に組み込まれた暗号鍵で暗号化して受信者端末へ送付し、前記受信者端末は、送付された暗号化データを一時的データ保管領域に保存し、該受信者端末内に組み込まれた復号鍵を用いて暗号化データを受信者に知られない方法で復号後、復号された送付データに対して署名用秘密鍵で電子署名を生成し、これを受領証として前記データ送信サーバへ返送し、前記データ送信サーバは、受理した受領証が送付データに対する受信者の電子署名であることを認証機関から取得した受信者の公開鍵証明証により確認して受領証を保存し、受領証を受領したことを示す受領証受理確認通知を前記受信者端末へ送付し、前記受信者端末は、前記データ送信サーバからの受領証受理確認通知を受領後、一時的データ保管領域に保管した暗号化データを再度復号鍵により復号し、復号された送付データを送付データ保管領域に保存することにより、データ送信サーバが、受信者端末から送付データを受領したことを証明する電子署名を受領証として受け取らない限り、受信者端末が受理した送付データの内容を確認することができないようにしたことを特徴とする電子データ配送方法。

【請求項3】 請求項2記載の電子データ配送方法において、前記受信者端末が受領証受理確認通知を受領でき

なかった場合に、前記受信者端末から再度前記データ送信サーバへ前記受領証を送り、前記データ送信サーバから受領証受理確認通知を再送してもらい、送付データの保管および内容の確認が可能になるようにしたことを特徴とする電子データ配送方法。

【請求項4】 コンピュータネットワークを介して、データ送信サーバから暗号化した電子データを受信する受信者端末であって、データ送信サーバから受信した暗号化データを一時的データ保管領域に一時的に保管するデータ受理手段と、受信者に知られない方法により組み込まれた復号鍵を用いて、受信者が内容を確認できない態様で前記受理した暗号化データを復号し、復号された送付データに対して、受領証となる電子署名を生成するための署名用秘密鍵を用いて受領証を作成し、前記データ送信サーバへ返送する受領証返送手段と、前記データ送信サーバから受領証受理確認通知を受け取った後に、前記暗号化データを復号鍵を用いて復号し、受信者が内容を確認できる態様で送付データ保管領域に復号した送付データを保管するデータ保管手段とを備えることを特徴とする電子データの受信者端末。

【請求項5】 コンピュータネットワークを介して確かに電子データを送付したことの証拠情報を、送信者が受信者から受け取るための電子データ配送システムにおける受信者端末を実現するためのプログラムを記録した記録媒体であって、データ送信サーバから受信した暗号化データを一時的データ保管領域に一時的に保管する処理と、受信者に知られない方法により組み込まれた復号鍵を用いて、受信者が内容を確認できない態様で前記受理した暗号化データを復号し、復号された送付データに対して、受領証となる電子署名を生成するための署名用秘密鍵を用いて受領証を作成し、前記データ送信サーバへ返送する処理と、前記データ送信サーバから受領証受理確認通知を受け取った後に、前記暗号化データを復号鍵を用いて復号し、受信者が内容を確認できる態様で送付データ保管領域に復号した送付データを保管する処理とを、計算機に実行させるプログラムを記録したことを特徴とする電子データの受信者端末用プログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータネットワーク上でEDI（電子データ交換）やEC（電子商取引）を実現するために必要となる電子データの配送システムにおいて、送信者が、受信者への電子データの送付と引き換えに、受信者から電子データを受領したことの証拠情報を受け取るためのシステムに関するものである。

【0002】

【従来の技術】図6は、従来技術による電子データの送付に対する受領証の受け取り方法を示したものである。

【0003】コンピュータネットワークを介して確かに電子データを送付したことの証拠情報を、送信者が受信者から受け取って保管しておきたい場合に、図6に示すように、送信者が送付対象データを作成して（S91）、受信者がこの送付した電子データを受理したら（S92）、受理した電子データに対する電子署名を生成してもらい（S93）、受信者にその生成した電子署名を受領の証として送付してもらって（S94）、送信者がこれを受け取る（S95）、という方法が考えられる。

【0004】電子署名は、RSAやESIGNなどの公開鍵暗号を用いて実現される技術であり、電子データの保持者のみが所有する秘密鍵を用いて、署名対象の電子データを暗号化することにより生成されるため、署名者が署名対象の電子データを保持していたことの証拠情報となりうる。

【0005】

【発明が解決しようとする課題】しかし、送信者が、電子データの送付と引き換えに、受信者からその電子データに対する電子署名を受領証として受け取りたい場合に、従来技術を用いると以下に示すような課題がある。

【0006】受信者端末には、受信者が電子署名を生成する前に電子データが保存されるため、受信者が電子データの内容を確認後に意図的に受領証の返送を中止したり、受領証の返送中に通信路に障害が発生した場合には、受信者が電子データを受領しているにもかかわらず送信者が受領証を受け取ることができないという問題である。

【0007】

【課題を解決するための手段】上記の課題を解決するため、本発明では、送信者が、受信者から送付データを受領したことを証明する電子署名を受領証として受け取らない限り、受信者が受領した送付データの内容を確認することができないことを特徴とした電子データ配送システムを提示する。以下において、本発明におけるシステム構成および本発明を実現するための手段について、図1、図2を用いて説明する。

【0008】図1は、本発明のシステム構成例を示す図である。本発明のシステムは、データ送信サーバ10、受信者端末20、認証機関（CA）30から構成される。

【0009】〔データ送信サーバ〕データ送信サーバ10は、組み込まれた暗号鍵14を用いて送付データを暗号化し、これを受信者端末20へ送付するためのデータ送付手段11と、受信者端末20からの受領証を受け取るための受領証確認手段12と、受領証を受領したことを受信者端末20へ通知するための受領証受理確認通知手段13から構成される。

【0010】〔受信者端末〕受信者端末20は、データ送信サーバ10から送付された暗号化データをディスク

上の一時的データ保管領域24に保管するためのデータ受理手段21と、受信者に知られない方法により組み込まれた復号鍵26を用いて暗号化データを復号し、復号された送付データに対して受信者のみが知りうる署名用秘密鍵27を用いて電子署名を生成し、この電子署名を受領証としてデータ送信サーバ10へ返送するための受領証返送手段22と、受信者が指定するディスク上の送付データ保管領域25に送付データを保管するためのデータ保管手段23から構成される。

10 【0011】〔認証機関（CA）〕認証機関（CA）30は、受信者が署名用秘密鍵27と対で作成した署名用公開鍵を受信者から受け取り、それに対する公開鍵証明書31を作成して保持する。

【0012】図2は、本発明を実現する手段およびその処理の流れを示す図である。

ステップS1：データ送信サーバ10のデータ送付手段11は、本手段に組み込まれた暗号鍵14を用いて送付データを暗号化し、その暗号化された電子データを受信者端末20へ送付する。

20 【0013】ステップS2：受信者端末20のデータ受理手段21は、ステップS1の処理で暗号化された送付データを受領し、これをディスク等の記憶装置上の一時的データ保管領域24に保管する。

【0014】ステップS3：受信者端末20の受領証返送手段22は、ステップS2の処理で保管した暗号化された送付データを本手段に組み込まれた復号鍵26により復号し、復号された送付データに対して、受信者の署名用秘密鍵27を用いて電子署名を生成する。そして、これを受領証としてデータ送信サーバ10へ返送する。

30 本手段は、電子署名を生成する過程において、復号された電子データの一部あるいは全ての情報に、受信者がアクセスできないように実現される。

【0015】ステップS4：データ送信サーバ10の受領証確認手段12は、ステップS3の処理で送付された受領証を受領し、これが送付データに対する受信者の電子署名であることを、認証機関（CA）30から取得した受信者の公開鍵証明書31を用いて確認し、その受領証を保存する。

40 【0016】ステップS5：データ送信サーバ10の受領証受理確認通知手段13は、ステップS4の処理の受領証の確認が終了した後、受領証を確かに受領したことを受信者端末20へ通知する。

【0017】ステップS6：受信者端末20のデータ保管手段23は、ステップS5の処理で送付された受領証受理確認通知を受領後、ステップS2の処理で一時的データ保管領域24に保管した暗号化された送付データを、受領証返送手段22に組み込まれた復号鍵26を用いて復号し、復号された送付データを受信者が指定したディスク等の記憶装置上の送付データ保管領域25に記録するとともに、一時的データ保管領域24に保管され

ていた暗号化されたデータを削除する。また、通信路の障害等により受領証受理確認の通知が受理できなかった場合には、受領証がデータ送信サーバ 10 に到達していない可能性があるため、上記ステップ S 3 の処理以降を再度実行し、データ送信サーバ 10 に受領証受理確認通知を送付してもらう。

【0018】以上に示した手段による処理の流れにより、データ送信サーバ 10 が受信者端末 20 から受領証として送付データに対する受信者の電子署名を受理するまで、受信者端末 20 において送付データの内容を受信者が確認できないようにすることが可能になる。

【0019】以上の各処理手段を計算機によって実現するためのプログラムは、計算機が読み取り可能な可搬媒体メモリ、半導体メモリ、ハードディスクなどの適当な記録媒体に格納することができる。

【0020】

【発明の実施の形態】本発明を実現するための具体的な実施の形態について、図 3 ないし図 5 を用いて説明する。図 3 は、本実施の形態におけるシステム構築時の処理の例を説明するための図、図 4 および図 5 は、本実施の形態におけるデータ送受信時の処理の例を説明するための図である。

【0021】最初に、図 3 に従ってシステム構築時の処理について説明する。

(a 1) 暗号鍵・復号鍵の生成

受信者に知られない方法により、暗号鍵をデータ送信サーバ 10 に、復号鍵を受信者端末 20 に組み入れるため、信頼できる第三者または送信者の端末 40 は、暗号鍵生成部 401 の機能を用いて暗号鍵 14 と復号鍵 26 を生成し、暗号鍵 14 をデータ送付手段 11 に、復号鍵 26 を受領証返送手段 22 とデータ保管手段 23 に組み入れる。暗号鍵生成部 401 は、例えば既存の暗号ソフトウェア等により実現されている乱数発生機能を用いて実現可能である。

【0022】(a 2) 暗号鍵・復号鍵のシステムへの組み込み

次に、信頼できる第三者または送信者の端末 40 は、ファイル配送部 402 の機能を用いて、(a 1) で生成したデータ送付手段 11 をデータ送信サーバ 10 へ配布し、受領証返送手段 22 とデータ保管手段 23 を受信者端末 20 へ配布して、これらをそれぞれでインストールしてもらう。ファイル配送部 402 は、例えば FTP などを用いて実現可能である。なお、例えば信頼できる第三者または送信者の端末 40 から、復号鍵を組み入れた受領証返送手段 22 とデータ保管手段 23 を個別に送るのではなく、データ受理手段 21、受領証返送手段 22 およびデータ保管手段 23 を実現するプログラムまたはスクリプトをまとめて、受信者端末 20 へ送るようにしてもよい。

【0023】また、信頼できる第三者または送信者の端

末 40 から、復号鍵を受領証返送手段 22 およびデータ保管手段 23 に組み入れて送る代わりに、復号鍵のみを暗号化などして受信者端末 20 へ送り、あらかじめ受信者端末 20 にインストールされた受領証返送手段 22 およびデータ保管手段 23 内に、受信者に認知できない方法で復号鍵を復号し組み入れる方法を用いてもよい。

【0024】(c 1) 受信者の署名用秘密鍵の生成
受信者端末 20 は、署名用鍵対生成部 201 の機能を用いて署名用秘密鍵 27 と公開鍵 28 の鍵対を生成し、署名用秘密鍵 27 は受信者端末 20 に保存し、公開鍵 28 は (c 2) の処理に用いる。署名用鍵対生成部 201 は、署名アルゴリズムに応じた秘密鍵 27 と公開鍵 28 のペアを生成する機能として、既存の暗号ソフトウェア等により実現されており、容易にこれを利用可能である。

【0025】(c 2) 受信者の署名用公開鍵の認証機関 (CA) への登録

上記 (c 1) で生成された鍵対のうち、データ送信サーバ 10 が電子署名を検証する際に公開鍵 28 を参照できるように、公開鍵登録依頼部 202 の機能を用いて、公開鍵の認証機関である認証機関 (CA) 30 へ公開鍵 28 を登録する。公開鍵登録依頼部 202 は、例えば認証機関 (CA) 30 が提供する公開鍵登録サービスを利用することにより実現可能である。

【0026】(d 1) 公開鍵証明証の作成

認証機関 (CA) 30 は、(c 2) で依頼された公開鍵 28 に対して、公開鍵証明証発行部 301 の機能を用いて受信者の公開鍵証明証 31 を作成し、これを認証機関 (CA) 30 内に保管する。公開鍵証明証発行部 301 の機能は、公開鍵に対してその所有者や有効期限など証明する公開鍵証明証を作成する機能であり、既存の認証機関 (CA) システムにおいて実現されている機能である。

【0027】データ送信サーバ 10 と受信者端末 20 との間でデータ送受信は、例えば図 4 および図 5 に示すように行われる。

【0028】[1] 受信者端末 20 へのデータの送付 (データ送信サーバ 10)

データ送信サーバ 10 のデータ送付手段 11 は、ファイルアクセス部 111 の機能を用いて、受信者へ送付するデータを読み出し (S 11)、データ暗号化部 112 の機能を用いて、データ送付手段 11 に組み込まれている暗号鍵 14 により送付データを暗号化する (S 12)。そして、データ通信部 113 の機能を用いて、暗号化された送付データ 71 を受信者端末 20 へ送付する (S 13)。ファイルアクセス部 111 は、コンピュータシステムで一般に提供されている機能であり、容易に利用可能である。また、データ暗号化部 112 は、暗号鍵 14 と暗号化したいデータを入力として暗号化データを出力する機能であり、既存の F E A L や D E S などの暗号技

術を用いて容易に実現可能である。データ通信部 113 は、例えば TCP/IP 通信などが利用可能であり、一般のコンピュータシステムにおいて実現されている機能である。

【0029】〔2〕暗号化された送付データの受理（受信者端末 20）

受信者端末 20 のデータ受理手段 21 は、データ通信部 211 の機能を用いてデータ送信サーバ 10 からの暗号化された送付データ 71 を受信し（S21）、ファイルアクセス部 212 の機能を用いてこれをディスク等の記憶装置上の一時的データ保管領域 24 へ記録する（S22）。

【0030】〔3〕受領証の作成・返送（受信者端末 20）

受信者端末 20 の受領証返送手段 22 は、ファイルアクセス部 221 の機能を用いて、上記〔2〕の処理で保管した暗号化データを読み出し（S31）、データ復号化部 222 の機能を用いて、受信者端末 20 に組み込まれている復号鍵 26 により暗号化データをメモリ上に復号する（S32）。続いて、メモリ上に復号された送付データに対して、ハッシュ化部 223 の機能を用いてハッシュ値を生成し、このハッシュ値に対して署名生成部 224 の機能を用いて、受信者の署名用秘密鍵 27 により電子署名を生成し、これを受領証 72 とする（S33）。そして、最後にデータ通信部 225 の機能を用いて、この受領証 72 をデータ送信サーバ 10 へ返送する（S34）。データ復号化部 222 は、暗号化データと復号鍵を入力として復号結果を出力する機能であり、データ暗号化部 112 と対になる機能として既存の暗号技術を用いて容易に実現可能である。ハッシュ化部 223 として、例えば SHA-1 や MD5 などのアルゴリズムが、ハッシュ値を暗号化し署名を生成する署名生成部 224 として、例えば E-SIGN や RSA などのアルゴリズムが広く知られており、どちらも既存の暗号ソフトウェア等により実現されており、容易に利用可能である。

【0031】また、本手段における電子署名を生成する過程（S31～S33）の各処理において、復号された送付データ 71 の情報は、ディスク等の記憶装置上に書き込まれないため、端末の障害等の発生により処理が中断して電子署名が生成されなかった場合でもその情報が残らず、受信者が送付データ 71 の内容を確認することはできない。

【0032】〔4〕受領証の確認（データ送信サーバ 10）

データ送信サーバ 10 の受領証確認手段 12 は、まず、データ通信部 121 の機能を用いて、上記〔3〕の処理で送付された受領証 72 を受理する（S41）。次に、受理した受領証 72 が、送付データ 71 に対して受信者が生成した電子署名であることを検証するため、電子署名の検証に必要な受信者の公開鍵証明証 31 を、公開鍵

取得部 122 の機能を用いて認証機関（CA）30 から取得し（S42）、送付データ 71 をファイルアクセス部 123 の機能を用いて再度取得した後（S43）、署名検証部 124 の機能を用いて電子署名の検証を行い、その正当性を判定する（S44）。そしてこの検証の後、受領証 72 をファイルアクセス部 125 の機能を用いて保存する（S45）。

【0033】公開鍵取得部 122 は、受信者の公開鍵を認証機関（CA）30 から取得する機能であり、例えばディレクトリ参照機能を用いて実現可能である。署名検証部 124 は、電子署名、署名者の公開鍵 28、署名対象データを入力として、電子署名が署名対象データに対して署名者の署名用秘密鍵 27 により生成されたことを確認する機能であり、署名生成部 224 と対となる機能として既存の暗号ソフトウェア等により実現されており、容易に利用可能である。

【0034】〔5〕受領証受理の確認通知（データ送信サーバ 10）

データ送信サーバ 10 の受領証受理確認通知手段 13 は、上記〔4〕の処理の受領証の確認が正常に終了した後、ファイル編集部 131 の機能を用いて受領証を受理したことを受信者端末 20 へ通知するための受領証受理確認通知 73 を作成し（S51）、これをデータ通信部 132 の機能を用いて受信者端末 20 へ送付する（S52）。ファイル編集部 131 は、例えばエディタ機能を用いるなど、通常のコンピュータシステムが提供する機能を用いることで実現でき、容易に利用可能である。

【0035】〔6〕データの保管（受信者端末 20）

受信者端末 20 のデータ保管手段 23 は、データ通信部 231 の機能を用いて、上記〔5〕の処理で送付された受領証受理確認通知 73 を受理した後（S61）、ファイルアクセス部 232 の機能を用いて、上記〔2〕の処理で一時的データ保管領域 24 に保管した暗号化データを読み出し（S62）、データ復号化部 233 の機能を用いて、受信者端末 20 に組み込まれた復号鍵 26 により暗号化データを復号し（S63）、ファイルアクセス部 234 の機能を用いて、復号化された送付データ 71 を受信者が指定したディスク等の記憶装置上の送付データ保管領域 25 に保管するとともに、保管されていた暗号化データを削除する。また、一定時間経っても受領証受理確認通知 73 が受理できない場合には、一時的データ保管領域 24 に保管されている暗号化データに対して、〔3〕以降の処理を再度繰り返す。

【0036】以上に示した処理を実現することにより、受信者端末 20 のディスク等の記憶装置上には、データ送信サーバ 10 が受信者端末 20 から受領証として送付データ 71 に対する受信者の電子署名を受理するまで、復号された送付データ 71 が書き込まれないため、受信者が受領証を返送せずに送付データの内容を確認することの防止が可能になる。

(受信者端末側)を説明するための図である。

【図6】従来技術による電子データ送付方法を示す図である。

10 データ送信サーバ

1.2 受領証確認手段

1.3 受領証受理確認

1.4 暗号鍵

20 受信者

2.1 データ受理

2.2 受領証返送手段

2.3 データ保管手段

2.4 一時的データ保管領域

2.5 送付データ保管領域

2.6 復号鍵

2.7 署名用秘密鍵

30 認証機関 (CA)

3.1 受信者の公開鍵証明証

【図 1】 本発明のシステム構成例を示す図である。

【図 2】本発明を実現する手段およびその処理の流れを示す図である。

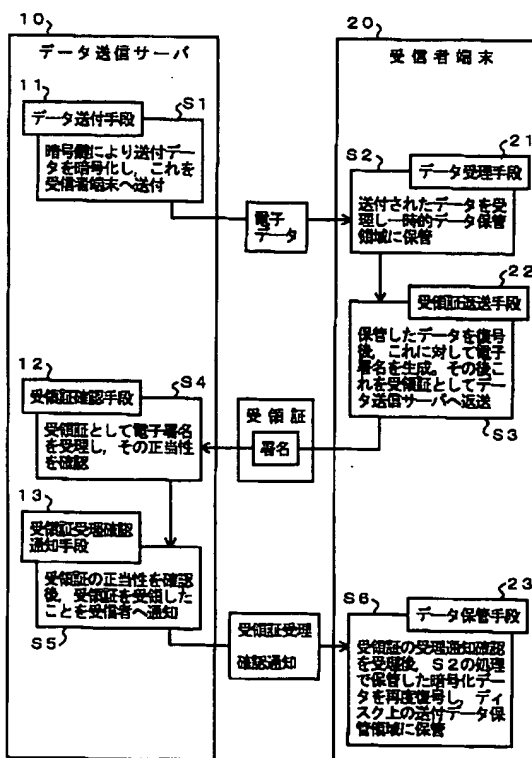
【図 3】本実施の形態におけるシステム構築時の処理を説明するための図である。

【図 4】本実施の形態におけるデータ送受信時の処理（データ送信サーバ側）を説明するための図である。

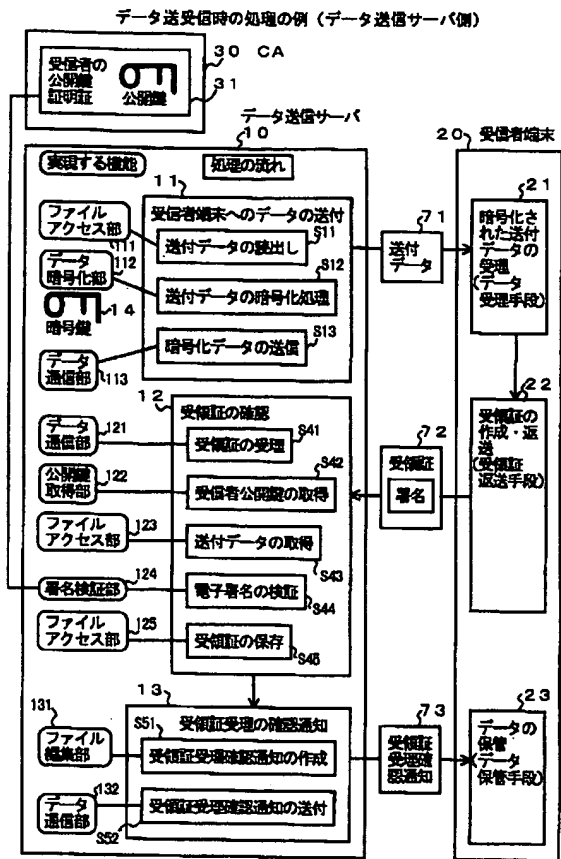
【図5】本実施の形態におけるデータ送受信時の処理

【图2】

本発明を実現する手段およびその処理の流れ

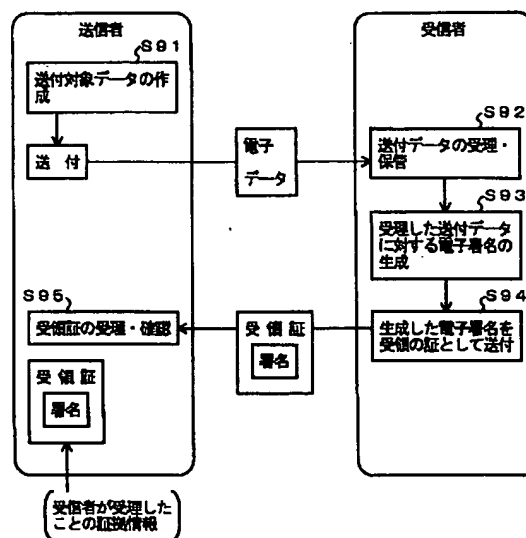


【図 4】



【图 6】

従来技術による電子データ送付方法



F ターム(参考) 5B085 AE06 AE13 AE29 CA04
5J104 AA01 AA09 EA16 JA21 LA06
NA02 PA07 PA10
9A001 EE03 JJ65 JJ67 LZ03

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.